UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH MaineHunter1991@GMAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE, INC.	Docket No. 1:20-mj- 126-01-AJ **Filed Under Seal – Level I**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Kristi R. McPartlin, a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF"), being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I submit this affidavit in support of an application for a warrant for information associated with a certain account that is stored at premises owned, maintained, controlled or operated by Google, Inc. an electronic communications service/remote computing service provider headquartered at 1600 Amphitheater Parkway, Mountain View, California ("Google"). The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google Inc. to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, and copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am currently employed as a Special Agent with the Bureau of Alcohol, Tobacco,

Firearms and Explosives ("ATF") and have been so employed since 2002. In the course of participating in investigations of firearms trafficking, I have conducted or participated in surveillance, the purchase of firearms, the execution of search warrants, debriefings of subjects, witnesses, and informants and reviews of consensually recorded conversations and meetings. Through my training, education, and experience, I have become familiar with the manner in which individuals and firearms traffickers use the internet, social media and email to buy, sell and trade firearms.

3. I am a "Federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 922 (a)(1)(A) has been committed by Brent BOUDREAU. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 922 (a)(1)(A).

STATUTORY AUTHORITY

7. Title 18, United States Code, § 922(a)(1)(A) makes it unlawful for any person, except a licensed importer, licensed manufacturer, or licensed dealer, to engage in the business of importing, manufacturing, or dealing in firearms, or in the course of such business to ship, transport or receive any firearms in interstate or foreign commerce. Title 18, United States Code § 921(a) defines "to engage in the business of" as devoting time, attention, and labor to dealing in firearms as a regular course of trade or business with the principle objective of livelihood and profit through the repetitive purchase and resale of firearms. This does not include a person who makes an occasional sale, exchange or purchase of firearms for the enhancement of a personal collection or a hobby.

PROBABLE CAUSE

8. This investigation arises out of the recovery by law enforcement in the Commonwealth of Massachusetts of a firearm originally purchased by Brent BOURDEAU. Specifically, on or about July 15, 2019, Quincy Police Department (MA) recovered a firearm described as a Glock, Model 19, 9mm pistol bearing serial # PFL464 during the events following an attempted traffic stop. An ATF Trace of the firearm revealed that BOUDREAU purchased this firearm at a Federal Firearms Licensee (or "FFL") in New Hampshire on May 4, 2019, approximately 70 days prior to the gun's recovery in Massachusetts.

9. The firearm was test fired and placed into the National Integrated Ballistic Information Network (NIBIN) by the Massachusetts State Police. The test fire revealed that there was a possible correlation between the recovered firearm and three prior incidents: an Assault with a Deadly Weapon in Worcester, MA, a Homicide in Worcester, MA and a Homicide in

Fitchburg, MA. All three incidents occurred following BOUDREAU's purchase of the firearm on or about May 4 and the recovery of the gun on or about July 15.

10. The Assault with a Deadly Weapon in Worcester was an incident where the victim survived a gunshot wound to the chest. This incident occurred on June 22, 2019. This would have made the time from when BOUDREAU purchased the firearm to the incident in Worcester approximately 47 days.

11. I have learned that BOUDREAU has purchased approximately 26 firearms from Federal Firearms Licensees ("FFL's") in New Hampshire from December 2018 through August 2019.

12. During an interview with BOUDREAU on August 12, 2019, I learned that BOUDREAU regularly sold and traded firearms on the website Armslist.com. BOUDREAU utilized his personal email account of Brentboudreau1991@gmail.com to contact potential purchasers and sellers. Armslist.com is an online website where firearms, firearms parts and firearms accessories are listed for sale and/or trade. I also learned that BOUDREAU was no longer in possession of any of the approximate 26 firearms he had purchased starting in December 2018. While BOUDREAU denied any illegal arms dealing, he could not tell me who he sold and/or traded any of the firearms to because he did not keep any paperwork for any of the transactions.

13. On August 14, 2019, a grand jury subpoena was issued to Armslist, LLC for online activity involving any accounts associated with Brentboudreau1991@gmail.com . On September 4, 2019, I began reviewing information received from Armslist.com.

14. According to Armslist, from May 2019 to August 2019, BOUDREAU was connected to approximately 144 gun listings. Of the 144 listings of firearms for sale, trade or

"offer". Of those listings, BOUDREAU had what appeared to be 53 firearms listed (meaning the firearms listed were duplicated or re-listed several times) for sale, trade or "offer" status. The majority of the approximate 53 firearms that BOUDREAU listed on the advertisements were for handguns, and many listings appear to overlap with the dates and time frames of when BOUDREAU purchased the firearms from FFLs. More specifically, an initial review of the listings show that approximately 16 of the firearms listed were similar to firearms purchased from Federal Firearms Licensees (FFLs) on the same day the firearms were purchased. (It is impossible to know for sure whether the listed firearms are the same as the purchased firearms without comparing serial numbers, but I have reached the conclusion based on a comparison of the firearm make, model and caliber.)

15. I served a search warrant for BOUDREAU's original email address Brentboudreau1991@gmail.com in January 2020. The email results came back with no results but showed that BOUDREAU deleted his account on September 13, 2019. A preservation order had been in place with Google but somehow the information got lost and deleted.

16. On or about March 2, 2020, ATF received information from an individual that showed purchases and sales from Armslist.com. The information came from an individual that had bought sold approximately 33 firearms utilizing the site through private sale. The individual provided ATF with copies of all emails pertaining to his sales and purchases. In the emails, the following new email addresses were being utilized by BOUDREAU: MaineHunter1991@gmail.com and MEhunter123@yahoo.com

17. ATF knows that the two above listed email address were being used by BOUDREAU because BOUDREAU sold one of his firearms in exchange for another listed in the email exchange (there are receipts with pictures of both parties NH State identifications)

using both email addresses dated September 7, 2019 at 8:52 PM (MEhunter123@yahoo.com) and 10:13 PM (MaineHunter1991@gmail.com).

18. In total, there are 14 conversations between BOUDREAU and the individual that provided ATF with the email communications and receipts. The first email conversation is dated August 30, 2019 and the last is dated September 24, 2019.

19. On or about April 21, 2020, Boston Police Department recovered a Glock GMBH, Model 19Gen4, 9mm pistol bearing serial # BKUW657 during the execution of a search warrant. This firearm was purchased by BOUDREAU on May 20, 2019 from a Federal Firearms Licensee (FFL) in Hooksett, NH. This firearm was entered into the NIBIN Enforcement Support System in Massachusetts. The firearm was given a high probability link to a shooting in Lynn, MA where (28) 9mm caliber casing were recovered at the crime scene. The shooting in Lynn, MA occurred on or about September 23, 2019. That makes the time to crime approximately 127 days from the time BOUDREAU purchased the firearm to the first time it is used in a crime of violence.

20. On or about May 20, 2020, the ATF NIBIN National Correlation and Training Center established a NIBIN lead between (11) s 9mm cartridge casings that were recovered in Lawrence, MA on August 21, 2019 in a shooting and a Glock, Model 17, 9mm pistol bearing serial # ACZD507 that was recovered in Lawrence, MA in a vehicle stop on October 6, 2019. BOUDREAU purchased the firearm from a Federal Firearms Licensee (FFL) in Hooksett, NH on July 11, 2019. This makes the time to crime for this firearm approximately 41 days from time of purchase to time of first shooting in Lawrence, MA.

21. From my experience and training, I know that individuals who buy firearms to resell them often purchase multiple units of the same caliber. I have learned that gun traffickers

acquire firearms in this manner to provide firearms to other states, countries, and to persons who cannot purchase firearms legally on the open market. In addition, I have learned through many investigations that individuals utilize online gun posting sites and auction sites to avoid completing an ATF Form 4473 for the firearms they purchase. Online posting sites also avoid a background check of the purchaser. If an individual attempts to purchase a handgun through a federally licensed firearms dealer (FFL), that person is required to complete ATF Form 4473, which documents the sale. ATF Form 4473 also triggers a background check on the purchaser to determine if the FFL may transfer the firearm to the purchaser. By using the website Armslist.com, BOUDREAU avoided having to pay a transfer fee to anyone he sold firearms to and also the purchasers avoided filling out an ATF Form 4473 for each firearm purchase and/or trade.

22. Based on my training and experience, the expedited purchase and sale/transfer of these firearms by BOUDREAU is indicative of the illegal dealing of firearms without a license. In particular, based on my training and experience, the listing for sale of firearms on or about the same day that they were purchased from an FFL- something I believe occurred on 16 separate occasions here- is indicative of the illegal dealing of firearms without a license.

23. While the Armslist records were voluminous, they ultimately do not tell the complete story of BOUDREAU's listings for sale or the completion of any transactions. Armslist confirmed their records reflect only listings and outgoing communications. Thus, any incoming messages BOUDREAU received from would-be purchasers would reside in the other email accounts he utilized to conduct firearms transactions, including MaineHunter1991@gmail.com.

24. In general, an email that is sent to a Google Inc. subscriber is stored in the subscriber's "mail box" on Google Inc.'s servers until the subscriber deletes the email. If the

subscriber does not delete the message, the message can remain on Google Inc.'s servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google Inc.'s servers for a certain period of time.

25. Based on the information set out above, I believe there is probable cause that Brent BOUDREAU used the email address MaineHunter1991@gmail.com to sell firearms he purchased at FFLs and to purchase multiple firearms from other Armslist users that he subsequently resold without a license.

BACKGROUND CONCERNING EMAIL

26. In my training and experience, I have learned that Google Inc. provides a variety of on-line services, including electronic mail ("email") access, to the public. Google Inc. allows subscribers to obtain email accounts at the domain name gmail.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with Google Inc. During the registration process, Google Inc. asks subscribers to provide basic personal information. Therefore, the computers of Google Inc. are likely to contain stored electronic communications (including retrieved and unretrieved email for Google Inc. subscribers) and information concerning subscribers and their use of Google Inc. services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

27. A Google Inc. subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google Inc. In my training and experience, evidence of who was using an email account may be found in address

books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

28. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

29. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

30. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

31. This application seeks a warrant to search all responsive records and information under the control of Google Inc. a provider subject to the jurisdiction of this court, regardless of where Google Inc. has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Google Inc.'s possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.[1]

32. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct

[1] It is possible that Google Inc. stores some portion of the information sought outside of the United States. In Microsoft Corp. v. United States, 2016 WL 3770056 (2nd Cir. 2016), the Second Circuit held that the government cannot enforce a warrant under the Stored Communications Act to require a provider to disclose records in its custody and control that are stored outside the United States. As the Second Circuit decision is not binding on this Court, I respectfully request that this warrant apply to all responsive information – including data stored outside the United States – pertaining to the identified account that is in the possession, custody, or control of Google Inc. The government also seeks the disclosure of the physical location or locations where the information is stored.

under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

FOURTEEN-DAY RULE FOR EXECUTION OF WARRANT

33. Federal Rule of Criminal Procedure 41(e)(2)(A),(B) directs the United States to execute a search warrant for electronic evidence within 14 days (formerly 10 days) of the warrant's issuance. If the Court issues this warrant, the United States will execute it not by entering the premises of Google, the company, as with a conventional warrant, but rather by serving a copy of the warrant on the company and awaiting its production of the requested data. This practice is approved in 18 U.S.C. § 2703(g),[2] and it is generally a prudent one because it minimizes the government's intrusion onto Internet companies' physical premises and the resulting disruption of their business practices.

34. Based on my training and experience and that of other law enforcement, I understand that e-mail providers sometimes produce data in response to a search warrant outside the 14-day period set forth in Rule 41 for execution of a warrant. I also understand that e-mail providers sometimes produce data that was created or received after this 14-day deadline ("late-created data").

35. The United States does not ask for this extra data or participate in its production.

36. Should Google, the company produce late-created data in response to this warrant, I request permission to view all late-created data, including subscriber, IP address, logging, and other transactional data, without a further order of the Court. This information could also be obtained by grand jury subpoena or an order under 18 U.S.C. § 2703(d), neither of

[2] Section 2703(g) provides that "[n]otwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service."

which contains a 14-day time limit. However, law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder(s), such as e-mail, absent a follow-up warrant.

CONCLUSION

37. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Google Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Dated: June 29, 2020

/s/ Kristi McPartlin
Kristi R. McPartlin
Special Agent
Bureau of Alcohol, Tobacco,
Firearms and Explosives

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Andrea K. Johnstone

Honorable Andrea K. Johnstone
United States Magistrate Judge
District of New Hampshire
Dated: **Jun 29, 2020**

ATTACHMENT A

Property to Be Searched

The premises to be searched and seized are (1) the email account identified as MaineHunter@gmail.com, (2) other user-generated data stored with those accounts, and (3) associated subscriber, transactional, user connection information associated with the accounts, as described further in Attachment B. This information is maintained by Google, Inc., which accepts service of process at:

1600 Amphitheatre Parkway

Mountain View, California 94043

Via Law Enforcement Portal: www.lers.google.com

ATTACHMENT B

Particular Things to Be Seized

I. Information to Be Disclosed by Google, Inc. (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and other files;

e. The contents of all text or instant messages

f. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

g. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.

II. Records and Data to Be Searched and Seized by Law Enforcement Personnel

For the period January 1, 2019, through the date of the search warrant, all information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of Title 18 United States Code § 922(a)(1), Unlicensed Dealing in Firearms, including, for the account listed on Attachment A, information pertaining to:

(a) The order, purchase, trade, or sale of firearms;

(b) The possession of firearms;

(c) Interactions with the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), including the application for, and/or acquisition of a Federal Firearms License;

(d) The use of the internet websites www.armslist.com, or any other website facilitating the sale of firearms or ammunition;

(e) Meetings between BOUDREAU and known or unknown persons regarding firearms purchases, sales, or transfers;

(f) Firearms licensing (state or federal) or any state or Federal laws or regulations relating to firearm sales;

(g) Communications between the Subject Account and other known or unknown persons regarding the unlicensed dealing of firearms;

(h) Travel in furtherance of unlicensed dealing of firearms;

(i) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(j) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(k) The identity of the person(s) who communicated with the Subject Account about matters relating to unlicensed dealing in firearms, including records that help reveal their whereabouts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Google, Inc. and my official title is _____. I am a custodian of records for Google, Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google, Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Google, Inc.; and

c. such records were made by Google, Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature